INTERNATIONAL SEARCH REPORT

International Application No
PCT/US 03/24000

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L9/32

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, WPI Data, PAJ, INSPEC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	HARN L: "Digital signature for Diffie-Hellman public keys without using a one-way function" ELECTRONICS LETTERS, IEE STEVENAGE, GB, vol. 33, no. 2, 16 January 1997 (1997-01-16), pages 125-126, XP006006945 ISSN: 0013-5194 the whole document ---	1,7, 9-14,21
X	SCHNEIER: "Applied cryptography." 1996 , JOHN WILEY & SONS. ISBN:0-471-11709-9 , NEW-YORK, US XP002276679 page 38, line 28 - line 37 ---	1,2,7, 9-15,21

-/--

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
13 April 2004	26/04/2004

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Dujardin, C

INTERNATIONAL SEARCH REPORT

International Application No
PCT/US 03/24000

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	GB 2 384 406 A (YEUN HYUN KU) 23 July 2003 (2003-07-23) abstract page 1, line 25 -page 4, line 1 page 4, line 20 -page 5, line 12 page 6, line 9 - line 21	1,2,14, 15
A	SCHNEIER: "Applied cryptography" 1996 , JOHN WILEY & SONS. ISBN:0-471-11709-9 , NEW-YORK, US XP002276680 cited in the application page 514, line 10 - last line	3,16
A	JOUX A: "A ONE ROUND PROTOCOL FOR TRIPARTITE DIFFIE-HELLMAN" ALGORITHMIC NUMBER THEORY, INTERNATIONAL SYMPOSIUM, XX, XX, vol. 1838, 2000, pages 385-393, XP008026749 page 387, line 26 -page 389, line 23	3,16
A	JINN-KE JAN ET AL: "A SECURE ANONYMOUS VOTING BY EMPLOYING DIFFIE-HELLMAN PKD CONCEPT" PROCEEDINGS OF THE 29TH. ANNUAL INTERNATIONAL CARNAHAN CONFERENCE ON SECURITY TECHNOLOGY. SANDERSTEAD, GB, OCT. 18 - 20, 1995, PROCEEDINGS OF THE ANNUAL INTERNATIONAL CARNAHAN CONFERENCE ON SECURITY TECHNOLOGY, NEW YORK, IEEE, US, vol. CONF. 29, 18 October 1995 (1995-10-18), pages 252-258, XP000585864 ISBN: 0-7803-2628-8 abstract page 252, right-hand column, line 14 - line 32 page 253, left-hand column, line 1 -right-hand column, line 11 page 254, left-hand column, line 20 -page 255, left-hand column, line 24 page 257, left-hand column, line 1 -right-hand column, line 13	1

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US 03/24000

Box I Observations where certain claims were found unsearchable (Continuation of item 1 of first sheet)

This International Search Report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. ☒ Claims Nos.: 22-24
because they relate to parts of the International Application that do not comply with the prescribed requirements to such an extent that no meaningful International Search can be carried out, specifically:
see FURTHER INFORMATION sheet PCT/ISA/210

3. ☐ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box II Observations where unity of invention is lacking (Continuation of item 2 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

1. ☐ As all required additional search fees were timely paid by the applicant, this International Search Report covers all searchable claims.

2. ☐ As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.

3. ☐ As only some of the required additional search fees were timely paid by the applicant, this International Search Report covers only those claims for which fees were paid, specifically claims Nos.:

4. ☐ No required additional search fees were timely paid by the applicant. Consequently, this International Search Report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest

☐ The additional search fees were accompanied by the applicant's protest.

☐ No protest accompanied the payment of additional search fees.

FURTHER INFORMATION CONTINUED FROM PCT/ISA/ 210

Continuation of Box I.2

Claims Nos.: 22-24

A meaningful search is impossible for independent claim 22 and for the dependent claims 23-24 which refer to it, due to the unclarity of the features of claim 22:

- Claim 22 claims a "device for generating digital signatures", but only defines method steps for generating public keys.
- It is unclear whether any link exists between these public keys and the signature device, since, in conventional signature schemes, SIGNATURE devices use PRIVATE keys to generate signatures, while PUBLIC keys are used by VALIDATION devices to validate the signature.
- Three different public keys are mentioned in claim 22 and it is unclear which purpose each of them serve and what is the link between them.
- According to claim 22, one of the three public keys is "transposed" from another one of the three public keys, but in the description (page 6, lines 11-15) on the other hand, the public key seems to be transposed from one of two PRIVATE keys. As a result, the description does not help interprete claim 22.

The applicant's attention is drawn to the fact that claims, or parts of claims, relating to inventions in respect of which no international search report has been established need not be the subject of an international preliminary examination (Rule 66.1(e) PCT). The applicant is advised that the EPO policy when acting as an International Preliminary Examining Authority is normally not to carry out a preliminary examination on matter which has not been searched. This is the case irrespective of whether or not the claims are amended following receipt of the search report or during any Chapter II procedure.

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/US 03/24000

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
GB 2384406 A	23-07-2003	WO 03063410 A1	31-07-2003